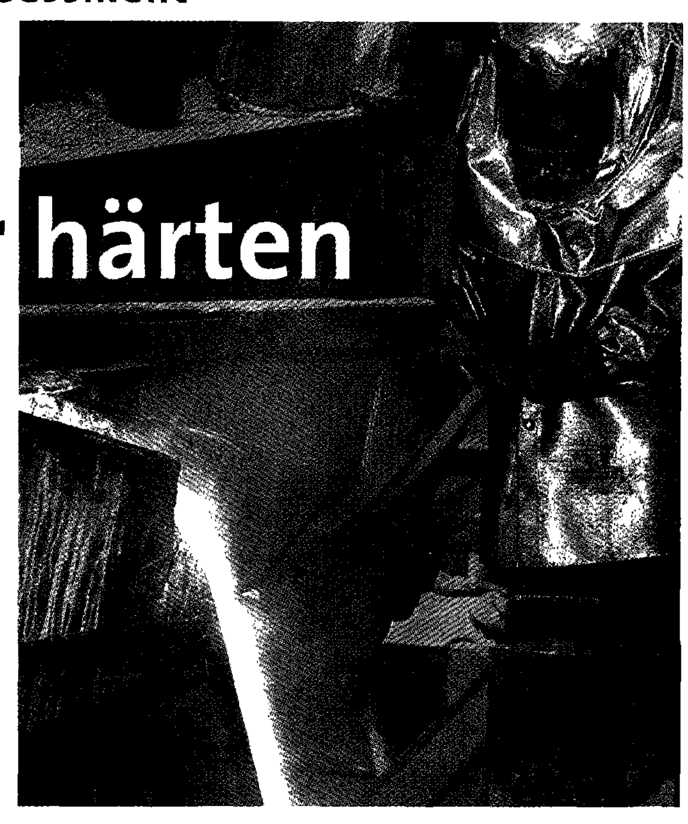
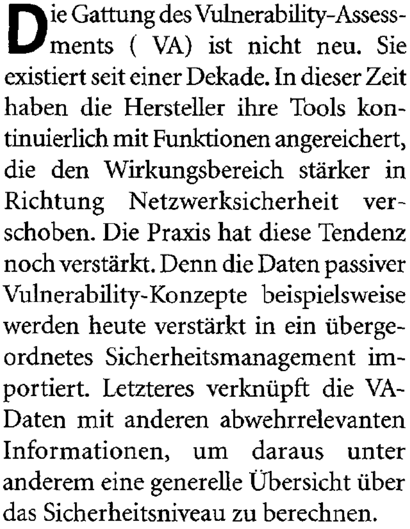
Suchwort:	Redaktion (Auflage):	Ausgabe (Datum):	Seite:	
QUALYS	INFORMATION WEEK SH (45.000)	1/06 (10.02.06)	1/3	

Werkzeuge zum Vulnerability-Assessment

Applikationen gegen Fehler härten



Schwachstellen in Clients und Servern zu finden und zu beheben, gehört aktuell zu einer der wichtigsten Abwehrmaßnahmen. Schreiben Cracker ihren Schadenscode doch hauptsächlich, um die Programmfehler auszunützen. Vulnerability-Assessment-Scanner spüren die Angriffspunkte auf, bevor es der Saboteur tut.



Die Gattung des Vulnerability-Assessments (VA) ist nicht neu. Sie existiert seit einer Dekade. In dieser Zeit haben die Hersteller ihre Tools kontinuierlich mit Funktionen angereichert, die den Wirkungsbereich stärker in Richtung Netzwerksicherheit verschoben. Die Praxis hat diese Tendenz noch verstärkt. Denn die Daten passiver Vulnerability-Konzepte beispielsweise werden heute verstärkt in ein übergeordnetes Sicherheitsmanagement importiert. Letzteres verknüpft die VA-Daten mit anderen abwehrrelevanten Informationen, um daraus unter anderem eine generelle Übersicht über das Sicherheitsniveau zu berechnen.

Die Entwicklungen in dem großen Vulnerability-Management-Bereich sind nicht losgelöst, sondern stark abhängig voneinander. Ohne passive Erkennungsmechanismen bleiben Vulnerabilties auf der Client-Seite aktiven Scannern eventuell verborgen. Eine Schwachstellen-Analyse ist insgesamt weniger effizient, wenn sie Daten anderer Quellen nicht importiert und auswertet. Die verschiedenen Disziplinen und Ansätze im Vulnerability-Assessment (VA) befruchten sich gegenseitig.

Strukturhilfen

Jeder große Themenbereich braucht Kategorien, damit er sich strukturieren und besser fassen lässt. Im VA-Segment wird einmal zwischen passiven und aktiven, einige sprechen gar von aggressiven Scannern unterschieden.

Der Begriff passiver Vulnerability-Scanner ist unglücklich gewählt, denn er verleitet zu einer falschen Annahme. Ein solcher Scanner scannt nicht. So wäre es angemessener, bei dieser Kategorie von einem Vulnerability-Detection-System zu sprechen. Viele Intrusion-Detection-Hersteller (IDS) haben letzteren Begriff allerdings schon mit Beschlag belegt. Nicht ohne Grund, denn in der Tat besitzen passive VA-Scanner und IDS-Produkte einige Gemeinsamkeiten: Beide beobachten passiv das Netzwerk, damit sie sicherheitsverletzende Daten aufspüren. Beide suchen dabei aber nach völlig unterschiedlichen Indikatoren. Während ein IDS nicht wenig überraschend nach Einbruchshinweisen (Intrusions) sucht, versucht ein passiver VA-Scanner, im Netzverkehr Hinweise auf existierende Vulnerabilities im Netz zu finden. Schwachstellen, die sowohl auf Client- als auch auf Serverseite liegen können.

Wie geschieht das? Der passive VA-Scanner erkennt beispielsweise einen Fehler im Browser, weil er in dessen User-Agent-String typische Merkmale aufspürt oder er ein verräterisches Verkehrsmuster im Netzverkehr erkennt. Solche Vulnerabilities würde ein konventioneller VA-Scanner nicht finden, außer der Administrator wiese ihm lokale Rechte auf dem jeweiligen Host zu.

Wie jedes System hat auch dieses Nachteile. Senden bestimmte Clients und Server keine Hinweise aus, verhalten sie sich also »still«, so wird der passive

VA-Scanner sie nicht aufspüren. Er ist darauf angewiesen, dass die zu untersuchenden Systeme aktiv Netzverkehr generieren und darin Hinweise auf die existierende Vulnerability geben. Hier sehen sich viele IDS-Hersteller äquivalent mit dem VA-Scannertypus. Denn auch ein IDS protokolliert einen Angriff oder eine ausgenutzte Schwäche, es unterbindet aber weder das eine noch das andere – wie ein passiver VA-Scanner. Allein deswegen ist es unwahrscheinlich, dass passive VA-Ansätze ihre aktiven Pendants jemals vollständig ersetzen können. Aktive wie passive Scanner können und sollten in einem Abwehrkonzept nebeneinander existieren.

Weise handeln

Die Effizienz der Vulnerability-Informationen ist daran gebunden, was mit ihnen geschieht. Schon eine einzige geschickt gewählte Anwendung kann aus einem dumpfen IDS-System ein intelligentes Tool formen. Wer beispielsweise ein automatisches System implementiert, das Informationen von verteilten Systemen sowie ihrer aktuellen Schwächen mit den gegen sie gerichteten Angriffen verknüpft, senkt beispielsweise die Anzahl von IDS-False-Positives deutlich.

VA-Checkliste

- Das VA-Tool muss in der Lage sein, sich gegenüber den existierenden externen Datenbanken zu authentifizieren.
- Das VA-Werkzeug sollte die Assets im Unternehmen verfolgen können.
- Der Administrator sollte die Größe der VA-Datenbank beachten und untersuchen, ob das VA-Produkt in für ihn wichtigen Software-Bereichen starke Checks beherrscht.
- Das gewünschte VA-System sollte in der Lage sein, den Patch-Status zu protokollieren.
- Bei der Kalkulation der Kosten sollten unbedingt auch die Lizenzgebühren für die VA-Updates berücksichtigt sein.

Zusätzlich kann eine ganze Reihe von Produkten wie der »VAM« von Stillsecure lokale Administratoren in großen Netzen aufspüren. Das Tool weist diesen Accounts außerdem IP-Ranges oder Hosts zu, für die die lokalen Administratoren dann verantwortlich sind.

Andere VA-Produkte arbeiten mit übergeordneten Management-Applikationen zusammen, um ebenso Verantwortlichkeiten oder Rechte zuzuweisen. Das »VA« von Tenable Network Security bindet sich beispielsweise in die Konsole von Lightning ein, der »SiteProtector« von ISS kann VA-Daten zusammenfassen und delegieren. Auf diese Weise können Administratoren ein unternehmensweites Vulnerability-Assessment-Konzept effizient und – wichtig – der allgemeinen Security-Policy entsprechend anwenden.

Große Unternehmen koppeln VA-Lösungen auch an externe Datenbanken, die deren Daten einmal archivieren, aber gleich nach Relevanz für den kritischen Geschäftsprozess gewichten, kategorisieren und in Workflow-Prozesse überführen. Das VA-Produkt autorisiert und authentifiziert die zentral archivierten Client- und Server-bezogenen Informationen und hält sie vor allem auf dem neuesten Stand.

Tiefer und weiter Ansatz

Einige VA-Systeme liefern auf Wunsch zahlreiche Details zu einer spezifischen Schwachstelle. Zusätzliche Informationen wie lokale Anwendernamen können beispielsweise beweisen, dass ein spezifischer Host zahlreiche Remote-Queries initiiert, aber niemals schließt. Solche Hintergrunddaten sind überzeugend. Der für die Datenbanken verantwortliche Kollege wird schnell verstehen, dass Schwachstellen auf Clientseite auch für ihn Folgen haben können. Jedes VA-Werkzeug liefert einige dieser Beweise. Ihre Detailtiefe ist abhängig von den Funktionen und dem Netz, in dem das Tool aktiv ist.

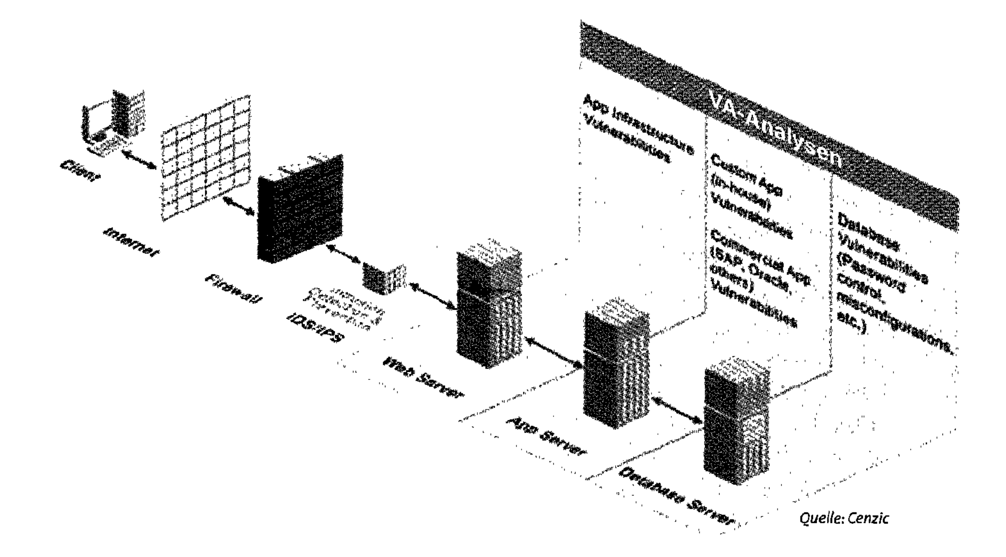
Wer ein VA-Tool einsetzen möchte, sollte auch einen Blick auf die Größe der Vulnerability-Datenbank werfen. Die pure Anzahl der gelisteten Schwachstellen ist dabei gar nicht ausschlaggebend, denn bestimmte Checks und Analysen sind für das eine Netz unverzichtbar, im anderen irrelevant. Eine reine Windows-Infrastruktur beispielsweise legt großen Wert auf alle Prüfroutinen, die sich auf diesen Softwaretypus konzentrieren. Wenn ein Produkt auf diesem Gebiet stark ist, in anderen wie Unix gegenüber der Konkurrenz abfällt, kann es dennoch das ideale Werkzeug für diesen individuellen Einsatzfall sein.

Ein anderer wichtiger Faktor sind die Zugriffsrechte, die ein VA für seinen Einsatz fordert. Viele VA-Lösungen schöpfen bereits existierende Administratorprivilegien aus, um sich remote in ein System einzuwählen und beispielsweise die Patchversion zu erfahren. Dies ist eigentlich eine Domäne der Patch-Management-Tools. Auf diesem Weg findet ein VA-Tool aber heraus, ob ein Host gewisse Schwachstellen besitzt, weil der eine oder andere Patch noch fehlt. Fehlen die lokalen Rechte, so sollte der VA-Scanner andere Remote-Checks beherrschen, die den Zugriffsmangel auf anderem Weg kompensieren.

Am Ende wollen die VA-Tools den Administrator informieren. Die Qualität dieser Inhalte ist an die Aussagekraft der Berichte gebunden. Wer die Reports selbst bearbeiten, in Details eintauchen möchte, sollte eine Lösung bevorzugen, die ihre Berichte entsprechend umgruppieren und aufwerten kann. Ein guter Vulnerability-Scanner interpretiert die gesamte Zahl der Schwachstellen übrigens in einen allgemeinen Graphen um, der wie ein Gesamtergebnis den Status quo in Netz wiedergibt. Im Idealfall sinkt der Wert im Betrieb, da die Verantwortlichen mit den VA-Daten Fehler finden und mit der Zeit ausmerzen konnten.

In der Praxis können VA-Scans auch Probleme verursachen, gerade bei älteren Betriebssystemen und Embedded-Devices. Sind im Netz mehrere kritische Plattformen aufgesetzt, die

zwingend verfügbar bleiben müssen, so sollte das VA-Produkt sanfte, vorsichtige Prüfroutinen beherrschen. Andere Bereiche im Netz verlangen sicher aggressivere Tests, sei es, um die Empfindlichkeit für einen Denial-of-Service-Attack zu untersuchen. Solche Tests bevorzugen die Holzhammermethode, denn sie trommeln mit Hunderttausenden von Paketen in der Sekunde auf das Zielsystem ein. Hier zeigt sich: Es ist immer ratsam, vorher zu wissen, was das VA-Tool untersuchen soll.



Quelle: Cenzic

Finden und reparieren

Was ein VA-Produkt am Ende auszeichnet? Es findet die Schwachstellen nicht nur, sondern hilft den Verantwortlichen dabei, diese zu beheben. Letztere Disziplin heißt passenderweise Remediation, auf deutsch Sanierung. Der Administrator sollte daher unbedingt einen Blick auf die vom gewünschten Tool gelieferten Remediation-Informationen werfen. Gerade bei Netzwerken, in denen die Serverpflege auf verschiedene Systemadministratoren mit wiederum individuellen Rechten verteilt ist, spielt die Qualität dieser Inhalte eine entscheidende Rolle. Denn sie helfen auch weniger erfahrenen Kollegen, den betroffenen Server zu reparieren und so die aufgedeckten Schwachstellen zu beheben.

Sind im Unternehmen starke Change-Kontrollmethoden etabliert, so werden sie die Last tragen, den Patchstatus zu protokollieren. Falls solche Prozesse fehlen, sollte das VA-Produkt diese Aufgabe beherrschen. Die meisten Produkte, die diese Disziplin abdecken, binden sich in der Regel in Security-Information-Management-Plattformen (SIM) ein.

Viele VA-Systeme werden nach Netzgröße und zu scannenden Hosts lizenziert. Wer ein großes Netz zu betreuen hat, in dem öfter IP-Adressräume hinzugefügt oder entfernt werden, sollte einen offenen Lizenzschlüssel kaufen. Er erlaubt es dem Administrator, jede beliebige Adresse zu untersuchen.

Wie Antivirusprodukte oder auf Signatur basierende IDS, sind VA-Produkte ohne permanente Updates nutzlos. Daher ist es ratsam, vor dem Kauf die Gebühren für die Aktualisierungen einzukalkulieren.

Passive und aktive VA-Scanner sind unter dem Strich wichtige Bestandteile eines Sicherheitsprogramms. Mit anderen Abwehrsystemen eingesetzt, helfen sie dabei, die Anfälligkeit gegenüber Angriffen zu reduzieren. Wer den größten Nutzen aus seinem VA-Konzept ziehen will, sucht am besten nach Integrationsmöglichkeiten in die übergeordneten Management-Lösungen. Ein VA-System, das diese Methoden unterstützt, wird sich am Ende immer bezahlt machen. *pm*

Kommerzielle VA-Angebote

Hersteller	Webseite
Altiris	www.altiris.com
Bindview	www.bindview.com
BMC	www.bmc.com
Cisco	www.cisco.de
Check Point	www.checkpoint.de
Computer Associates	www.ca.com
Enterasys	www.enterasys.com
Eeye	www.eeye.com
GFI Software	www.gfi.com
Harris	www.stat.harris.com
Hewlett-Packard	www.hewlett-packard.de
IBM/Tivoli	www.ibm.com
Internet Security Systems	www.iss.net
IP Locks	www.iplocks.com
Landesk	www.landesk.de
McAfee	www.mcafee.de
Symantec	www.symantec.de
Tenable Network Security	www.tenablesecurity.com
Telos Corporation	www.telos.com
Trend Micro	www.trendmicro.de
Qualys	www.qualys.de